CENTRO DE DIAGNÓSTICO AUTOMOTOR DE NARIÑO LTDA.

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

TABLA DE CONTENIDO

OBJETIVO GENERAL

Consolidar y fortalecer el Plan y Procedimiento de Tratamiento de Riesgos de Seguridad y Privacidad de la Información del CDA de Nariño, asegurando la eficacia de los controles implementados, la reducción del riesgo residual y la sostenibilidad de las medidas adoptadas durante la vigencia 2026.

OBJETIVOS ESPECÍFICOS

- Mantener controlados los riesgos identificados en el mapa de calor institucional acorde en el CDA.
- Verificar la eficacia de los controles técnicos, administrativos y físicos implementados, considerando su impacto en el cumplimiento normativo, la continuidad del negocio y la confianza de los clientes.
- Gestionar y monitorear el riesgo residual, que se define para mitigar, aceptar, transferir o evitar los riesgos identificados, en alineación con las mejores prácticas internacionales (ISO 27001 e ISO 27701).
- Realizar seguimiento y control a la eficacia del plan, mediante indicadores de desempeño, auditorías internas y revisiones periódicas, garantizando la mejora continua en la gestión de riesgos.

MARCO LEGAL

Norma	Descripción
Decreto 1078	Por medio del cual se expide el Decreto Único del Sector de Tecnologías de la Información y las Comunicaciones.
NTC / ISO 27001	Tecnología de la información. Técnicas de seguridad. Gestión de la seguridad de la información (SGSI).
NTC / ISO 31000:2009	Gestión del Riesgo. Principios y directrices.
MSPI (Modelo de Seguridad y Privacidad de la Información) MINTIC	entidades públicas colombianas implementen un Sistema de Gestión de Seguridad y Privacidad de la Información (SGSPI), basado en el ciclo PHVA (Planear, Hacer, Verificar, Actuar).

MARCO TEÓRICO

La técnica de análisis de riesgo aplicada a los activos de información del CDA de Nariño se orienta a identificar y gestionar los riesgos que pueden comprometer la seguridad, privacidad, y continuidad de los procesos operativos y administrativos. Desde un enfoque sistémico y alineado con los objetivos del negocio, este análisis incluye las siguientes áreas críticas:

- Identificación de puntos críticos de fallas en procesos clave, como reportes al RUNT y manejo de bases de datos.
- Análisis de disponibilidad, enfocado en garantizar la operación continua del CDA.
- Análisis de vulnerabilidad para detectar brechas en la infraestructura física y tecnológica.
- Análisis de confiabilidad de los sistemas utilizados en diagnósticos vehiculares y administración.

Para la vigencia 2026, el Plan de Tratamiento de Riesgos se fundamenta en la etapa de consolidación, posterior a la implementación de controles derivados del análisis del mapa de calor y la matriz de riesgos institucional. El enfoque del plan se orienta al seguimiento, evaluación de la eficacia de los controles y gestión del riesgo residual, alineado con el ciclo PHVA.

ENFOQUE PHVA PARA EL CDA DE NARIÑO

- **Planear**: Establecer políticas, objetivos y procedimientos para gestionar riesgos.
- **Hacer**: Implementar los controles definidos en el plan.
- **Verificar**: Monitorear y evaluar la eficacia de los controles mediante auditorías periódicas.
- **Actuar**: Realizar ajustes y mejoras continuas en el plan de tratamiento.

ACTIVIDADES GENERALES

Las actividades generales del plan son:

I. **Establecimiento del contexto**

- Definir los objetivos de seguridad y privacidad específicos del CDA.
- Identificar los procesos críticos del CDA, como la emisión de diagnósticos vehiculares y la gestión de datos personales.
- Revisión anual del contexto interno y externo.
- Identificación de cambios normativos, tecnológicos y operativos.

II. **Identificación de activos y riesgos asociados**

- Actualización del inventario de activos de información.
- Revisión de riesgos previamente identificados.
- **Activos principales**:
  - Base de datos de diagnósticos vehiculares.
  - Infraestructura tecnológica y conexiones con el RUNT.
  - Información personal y contractual de los clientes.
- **Riesgos asociados**:
  - Fuga de datos personales o resultados de diagnósticos.
  - Acceso no autorizado a sistemas.
  - Falta de actualizaciones en el software operativo.

III. **Estimación de riesgos**

- **Evaluación del riesgo residual**
- Reevaluación del nivel de riesgo considerando los controles implementados.
- Actualización del mapa de calor.

IV. **Tratamiento del riesgo**

- Mantenimiento de controles implementados.
- Documentación de riesgos aceptados.

- Implementar controles para mitigar riesgos críticos, como:
  - Cifrado de datos.
  - Controles de acceso basados en roles.
  - Auditorías regulares de seguridad.
- Definir un cronograma de implementación para las medidas.

V. **Aceptación del riesgo**

- Documentar los riesgos que no serán tratados activamente, explicando las razones y asegurando que el nivel de riesgo residual sea aceptable para la organización.

Adicional, el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información para el CDA de Nariño seguirá las actividades especiales adaptadas al contexto operativo y administrativo de la entidad, de la siguiente manera:

Programación y Agendamiento de Entrevistas

- Descripción: Se identifican los procesos críticos relacionados con el manejo de información del CDA, como la generación de diagnósticos vehiculares, la gestión de datos personales y la conexión con sistemas externos como el RUNT.
- Objetivo: Asegurar la participación de los responsables para identificar riesgos asociados a los procesos incluidos en el alcance del MSPI (Modelo de Seguridad y Privacidad de la Información) del CDA.

Entrevista con los Líderes de Proceso

- Descripción: Reuniones individuales o grupales con los líderes de cada proceso, facilitadores y personal operativo, donde:
  - Se explica la metodología de análisis de riesgos.
  - En conjunto, se identifican los riesgos asociados a los activos de información del proceso.

Identificación y Calificación de Riesgos

- Descripción: Evaluación de los riesgos identificados con base en:
  - Impacto: Nivel de daño que podría causar el riesgo en términos operativos, legales, financieros y de reputación.

- Probabilidad: Frecuencia con la que podría materializarse el riesgo.
- Controles existentes: Medidas actuales para mitigar el riesgo.

- Método: Uso de una matriz de probabilidad vs. impacto para asignar una calificación al nivel de riesgo.

Valoración del Riesgo Residual

- Descripción: Proyección del riesgo restante después de aplicar los controles actuales y los propuestos. Esto incluye:
  - Análisis de la eficacia de los controles existentes.
  - Ajuste de las calificaciones de riesgo basado en los controles implementados.
- Objetivo: Determinar si el nivel de riesgo residual es aceptable según los criterios del CDA.

Mapas de Calor donde se Ubican los Riesgos

- Descripción: Representación visual de los riesgos en un mapa de calor, donde:
  - Ejes: Probabilidad vs. Impacto.
  - Colores: Riesgos de nivel bajo (verde), medio (amarillo) y alto (rojo).
- Objetivo: Facilitar la priorización y el seguimiento de riesgos.

Plan de Tratamiento de Riesgos

- Descripción: Desarrollo de un plan detallado que incluya:
  - Controles específicos para mitigar cada riesgo.
  - Responsables para la implementación de controles.
  - Plazos y recursos necesarios.

Seguimiento y Control

- Descripción: Monitorear continuamente la implementación de controles y evaluar su eficacia mediante auditorías, revisiones periódicas y análisis de incidentes.

- Método:
  - Definir indicadores clave de desempeño

- Revisar y actualizar el plan de tratamiento según los resultados

CRONOGRAMA

Actividad	Descripción	Duración Estimada	Responsable
Programación y Agendamiento de Entrevistas para el año 2026	Identificación de procesos críticos y agendamiento de reuniones con líderes, facilitadores y personal operativo.	2 semana	Control Interno
Entrevista con los Líderes de Proceso y revisión de credenciales.	Reuniones con líderes y facilitadores para explicar la metodología y realizar el análisis de información proporcionada previamente	3 semanas	Control Interno
Monitoreo e Identificación de Riesgos	Evaluación de riesgos identificados en términos de impacto, probabilidad y controles existentes.	2 semana	Control Interno
Valoración del Riesgo Residual	Proyección del riesgo restante tras aplicar controles actuales y propuestos, evaluando su aceptabilidad.	2 semana	Control Interno
Capacitación en seguridad y privacidad de la información	Sensibilización y capacitación al personal del CDA sobre buenas prácticas de seguridad de la información y protección de datos personales.	3 semanas	Control interno
Mapas de Calor donde se Ubican los Riesgos	Visualización de riesgos priorizados en mapa de calor según impacto y probabilidad.	2 semana	Control Interno
Plan de Tratamiento de Riesgos	Desarrollo y aprobación del plan de tratamiento y seguimiento del documento existente.	3 semanas	Control Interno
Seguimiento y Control	Monitoreo y evaluación continua de la implementación de controles y resultados del plan.	Continuo (auditorías trimestrales)	Control Interno

GLOSARIO

- **Activo**: Cualquier recurso, bien o información que posea valor para la organización.
- **Análisis del riesgo**: Proceso de estimación del riesgo que proporciona las bases necesarias para evaluar su naturaleza e importancia.

- **Causa**: Factor específico que origina un evento de riesgo.
- **Contexto externo**: Entorno externo en el que opera la organización para alcanzar sus objetivos, incluyendo aspectos tecnológicos, legales, regionales, entre otros.
- **Contexto interno**: Entorno interno que abarca aspectos como el gobierno corporativo, políticas, estructura organizacional y cultura, en el cual la organización busca cumplir sus metas.
- **Controles**: Procesos, políticas y actividades diseñados para modificar o gestionar riesgos.
- **Criterios de riesgos**: Parámetros de referencia establecidos para evaluar la relevancia o gravedad de un riesgo.
- **Evaluación del riesgo**: Comparación entre los resultados del análisis de riesgo y los controles existentes, con el propósito de determinar el nivel de riesgo final.
- **Evento**: Potencial ocurrencia de un incidente o amenaza que pueda comprometer la seguridad de la información.
- **Fuente**: Elemento, tangible o intangible, que por sí solo o en combinación tiene el potencial intrínseco de generar riesgos.
- **Gestión del riesgo**: Conjunto de actividades coordinadas para dirigir y controlar la organización en relación con los riesgos.
- **Identificación del riesgo**: Proceso mediante el cual se determinan las causas, fuentes y eventos que, en función del contexto y del proceso, pueden afectar el cumplimiento de los objetivos organizacionales.
- **Riesgo aceptable**: Nivel de riesgo que la organización considera tolerable o manejable, de acuerdo con sus obligaciones legales, contractuales o intereses estratégicos.
- **Riesgo residual**: Riesgo que permanece después de implementar medidas de tratamiento.
- **Riesgo**: Posibilidad de que un evento afecte las funciones de la organización e impacte el cumplimiento de sus objetivos.

El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información del Centro de Diagnóstico Automotor de Nariño LTDA., para la vigencia 2026, se orienta a la consolidación, seguimiento y mejora continua de los controles implementados, como resultado del análisis de riesgos y del mapa de calor institucional previamente desarrollado. A través de este plan, la entidad garantiza la gestión adecuada del riesgo residual, el cumplimiento de los requisitos normativos aplicables y la protección de los activos de información, fortaleciendo la confidencialidad, integridad y disponibilidad de la información. La ejecución de las actividades definidas permitirá asegurar la continuidad del negocio, reforzar la cultura organizacional en seguridad de la información y mantener la confianza de los usuarios y partes interesadas.

JUAN CARLOS CABRERA ESTRADA
Gerente

1. ELABORACIÓN Y APROBACIÓN DE DOCUMENTOS.

Tabla 1.
Elaboración y aprobación de documentos

Elaborado:	**Revisado:**	**Aprobado:**
Se firma en original	**Se firma en original**	**Se firma en original**
Jefe de pista Suplente	Control interno	Gerente

2. REGISTRO DE CAMBIOS.

Tabla 2.
Registro de cambios.

Fecha	Versión	Descripción del cambio
2026-01-21	02	Se codifico documento.